DDC-TZ

DDC DIRECTIVE

NO. 5230.9   May 20 1999

            DDC INTERNET/INTRANET POLICY
      (Clearance of DoD/DDC Information for Public Release)

A. REFERENCES.

    1. DoD Directive 5200.4, "DoD Information Technology (IT) Security
        Certification and Accreditation (C&A) Process (DITSCAP)."

    2. DLA Internet Policy, dated 1 May 1997. The DLA policy on
        Dissemination and Obtaining Information Via the Internet and
        World Wide Web, Intranets and Electronic Mail.

    3. Deputy Secretary of Defense John Hamre's Web Security Policy, 24
        September 1998.

    4. DoD's Web Site Administration Policies and Procedures document
        25 November 1998.

    5. DoD 5230.9 "Clearance of DoD Information for Public Release
        9 April 1996.

B. PURPOSE.

   1. This directive implements current DoD and DLA policy. The World
Wide Web (WWW) is an open-ended information system designated
specifically with ease of use for documentation and informational
interchange in mind. Standards in place on Web (HTTP, FTP, ASP, etc.)
allow information to be transferred properly.

   2. The Web is built on existing protocols and is intended to provide
common interface to other protocols. The Defense Distribution Center
(DDC) web site will streamline customers support out, and cost of
publishing various information. The web site will offer quick access
to information, data, and allow interaction and feedback from users.
DDC will focus on delivering application services and site content to
DDC customers.

C. APPLICABILITY AND SCOPE.

    This policy is applicable to:

1. All employees of Defense Distribution Center Headquarters, DDC
   Distribution Depots, and Mapping Support Activities.

2. All unclassified DDC Web sites, both publicly and non-publicly
accessible.

D. DEFINITIONS.

World Wide Web - The subset of the Internet capable of providing the public with user-friendly graphics-based multi-media access to information on the Internet. It is the most popular means for storing and linking Internet-based information in all multi-media formats. Navigation is accomplished through a set of linked documents that may reside on the same computer or on computers located almost anywhere else in the world.

Web Browser - Application used to access pages and move throughout the World Wide Web. Two of the most popular browsers are Netscape Navigator and Microsoft's Internet Explorer. (The DDC Internet will support both browsers.)

Content Managers - The business area experts who develop the functionally related information that comprises the Web's content and who advises the PAO and Webmaster on its correctness.

Homepage - The index or introductory document for a Web site.

HTTP (HyperText Transfer Protocol) - Protocol, used by the World Wide Web which defines how messages are formatted and transmitted and what actions Web servers and browsers should take in response to various commands.

Firewall - A term for software which limits user access into and out of a network.

Internet - An informal collection of government, military, commercial, and educational computer networks used to transmit information electronically. This worldwide group of networks uses gateways to convert files to standard formats and protocols.

Intranet - A technological clone of the Internet, but access is restricted to an organization's internal audience and, by invitation, selected business partners.

E. POLICY. (General)

  1. The Internet provides the Defense Distribution Center and its components a new and powerful means to process and disseminate publicly releasable information. The DDC Commanders will strongly encourage its use as a business and communication tool to benefit DDC's mission accomplishment.

  2. DDC personnel and associated contractors are responsible for ensuring the safe, effective, efficient and legal use of government resources while using or posting to an Internet/Intranet.

  3. It is DDC policy to ensure that its employees/representatives:

    a. Exercise the highest standards of professional conduct and responsible behavior with the information they obtain from or make available to the Internet.

b. Defend the security of our nation and promote taxpayers' interests by exercising due caution and protecting information that unscrupulous contractors, foreign governments, or others might use to the disadvantage of the Department of Defense, or the U.S. Government. Examples of what must be protected include proprietary, contractual, operationally sensitive, and classified information.

c. Assume that anyone in the world can access the Internet and therefore take all necessary steps to preclude unauthorized disclosure of information.

d. Information placed on the Internet is subject to legal and regulatory requirements as non-electronic information. Requirements include compliance with Privacy Act, the Freedom of Information Act, copyright protection, and other laws.

e. Information must be formally reviewed and approved for release to the Internet in accordance with DoD Directive 5230.9, "Clearance of DoD Information for Public Release". The responsibility is assigned to the DDC Command Affairs Officer.

f. Ensure that reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Internet and Intranet.

g. Under no circumstance will classified information be placed on or made accessible by the Internet or unsecured Enterprise-wide Intranet.

F. RESPONSIBILITY.

 DDC POLICY ON INTERNET USE:

  1. OFFICIAL USE - Must be used in the interest of the DDC and the federal government. Such use should be appropriate in its frequency and duration and related to an employee's assigned duties.

  2. NON-OFFICIAL USE - DDC employees are authorized to use government computers to access the Internet for personal purposes. Employees should control the frequency and duration of the non-official usage to preclude any appearance of impropriety and unnecessary costs to the federal government. Incidental usage should occur on such personal time as breaks, lunch periods, and after-duty hours. Those who to not adhere to this policy will be subject to adverse personnel actions ranging from reprimands to suspension and dismissal.

 DDC POLICY ON INTERNET POSTING:

  1. Each DDC Distribution Depot and Mapping Support Activity's presence on WWW will be through a link on the DDC Internet Homepage.

  2. Posting to the Internet's global audience can only be allowed after permission from DDC Command Affairs Officer, and the Web Approval Board consisting of the Command Affairs Officer, DDC Webmaster, and others appointed by DDC Command. The Web Board will ensure compliance with DDC, DLA and DoD Policies and Directives.

DDC WEB APPROVAL BOARD:

1. DDC Web Approval Board will review and approve all information
and images to ensure security conformance and that proposed pages
reflect the professionalism of the DDC and its subordinate activities.
The checklist, shown as Enclosure 1, will be following for regulatory
compliance.

2. Requests for additions to the DDC Internet must be in writing (E-
mail is acceptable) to the Web Approval Board in the format as shown in
Enclosure 2. Request must outline: proposed content, the target
audience, point of contact, telephone and fax numbers, email address
and organization/office symbol.

3. As deemed appropriate, new requests, will be approved by Web
Board on case-by-case basis.

DDC CONTENT MANAGER:

1. Each Internet Page will be assigned a Content Manager, who will
be responsible for the correctness of the page content.

2. Content Managers will coordinate postings with the DDC WebMaster
to ensure compliance with DDC policy and hardware space availability.

DDC WEBMASTER:

1. Operate and maintain DDC Internet (http://www.ddc.dla.mil) as the
official primary point of access to DDC information on the Internet.

2. DDC Webmaster will serve as the technical consultant and provide
assistance to content managers on the implementation or posting of the
approved information.

3. All Internet pages will maintain the same look and feel approved
for the DDC Internet.

LOCAL AREA NETWORK (LAN)

The preferred avenue for using the Internet is through the
established Local Area Network. Should a business reason deem it
necessary to use an Internet Service Provider (ISP) to publish
information, approval from DDC Web Approval Board must be obtained
PRIOR to any publication. This will allow security assessments to
initially be accomplished to address any potential vulnerability. The
business reason, along with vulnerability assessment must be
documented. All requirements to use ISP, which are approved, will be
periodically reevaluated.
(Caution: Internet Service Providers are subject to the same sort of
slow-downs and related concerns, encountered with the LAN.)

DDC POLICY ON INTRANET USE:

1. The DDC Internal network (Intranet) will be accessible only to
DDC employees and selected outsiders, who have a valid Login and
Password or are allowed access through installed firewalls.

2. The DDC Intranet will be accessible by DDC employees and identified visitors from all networked DDC sites, but the "general public" will not be permitted to view its content.

     DDC POLICY ON INTRANET POSTING:

   1. The DDC Intranet (https://ddcnet.ddc.dla.mil), known as DDCnet, will be operated and maintained by the DDC Web Master as the official primary point of access.

   2. Posting to the Intranet, as with the Internet, can only be allowed after notifying the Web Approval Board, in writing, of its contents and purpose, for assurance with DoD, DLA and DDC compliance.

   3. Each DDC Directorate, Office, and Depot should appoint a Content Manager to update and maintain the correctness of the content of the pages within their assigned interests/jurisdiction. These pages must only be viewable to DDC audience or a subset thereof.

   4. The DDC Intranet will also allow all Distribution Depots and Mapping Support Activities to maintain their own local web pages, viewable to their own Depot/Office personnel. Space may be used on the DDC Intranet Server, if requested.

   5. The DDC Intranet Homepage will have a link from the DDC Internet Server.

   6. Any information/pages accessible to users outside the pre-defined boundaries of the DDC, become Internet items and must be approved by the DDC Web Approval Board, as such, and HOUSED on the DDC Internet Web Server.

G. EFFECTIVE DATE AND IMPLEMENTATION. This directive is effective and shall be implemented upon command signature and distribution.

H. INFORMATION REQUIREMENTS. Depot Commands will ensure that a copy of this publication is provided to all affected local unions.

BY ORDER OF THE COMMANDER.

                                    [Signed]

                                    GLENN M. MELTON
                                    Colonel, USA
                                    Chief of Staff

Encls.1. DDC Web Review Checklist
      2. DDC World Wide Web Page Request

DISTRIBUTION:
A + B
Depot Commands
Mapping Support Activities

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA	OFC	DATE
Defense Distribution Center Web Review Checklist		

NO.	ITEM	Y	N	N/A
1.	Has a security certification and accreditation package been accomplished for each organization establishing a Web site? Ref: DoD Policy, 25 Nov 98, Part II, para 2.2.	☐	☐	☐
•	**General Web Page Content**	☐	☐	☐
2.	Does the Web Page have a clearly defined purpose that supports the mission? Ref: DoD Policy, 25 Nov 98, Part II, para 2.1.			
3.	Have reasonable efforts been made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site? Ref: DoD Policy, 25 Nov 98, Part I, para 5.5.7.	☐	☐	☐
4.	Are Internet pages professionally presented, current, accurate, factual, and related to the organizational mission?	☐	☐	☐
5.	Is outdated or superseded information on each page identified and promptly removed from the system?	☐	☐	☐
6.	Does each page, as a minimum, contain Page OPR name, organization, office symbol, commercial phone number, DSN phone number, e-mail address, and any disclaimers or restrictions which apply to the page?	☐	☐	☐
7.	Has the Content Manager incorporated a feedback mechanism, which is easily accessible for users' comments?	☐	☐	☐
8.	Have individual pages only been developed when suitable for a specific duty position, such as organizational commanders? (Personal pages are normally inappropriate. Under no circumstances should the page extend beyond official duties and position)	☐	☐	☐
9.	Are CGI scripts only used when absolutely necessary, and only when thoroughly examined?	☐	☐	☐
	Specific Information Restrictions.			
10.	Is the following information prohibited from all web pages? SSANs, Dates of Birth, Home addresses, and other than duty office telephone numbers. Ref: DoD Policy, 25 Nov 98, Part II, para 3.5.3.4. (This includes publicly released base newspapers on the web.)	☐	☐	☐
11.	Are names, locations, and specific identifying information about family members of DoD employees and military personnel prohibited from all Web pages? Ref: DoD Policy, 25 Nov 98, Part II, para 3.5.3.5. (This includes publicly released base newspapers on the web.)	☐	☐	☐
12.	Is the following additional information excluded from publicly accessible DoD Web sites as appropriate? Official travel itineraries of individuals or units before performed, duty rosters, detailed organizational charts, directories with names, internal DoD personnel rules and practices unless cleared for release, information relating to A-76 studies and other outsourcing, and many other examples as contained in the reference. Ref: DoD Policy, 25 Nov 98, Part V, para 2. (This includes publicly released base newspapers on the web).	☐	☐	☐
13.	Are the following forms of information also prohibited from being placed on Web sites, either public or restricted? Classified information, Privacy Act information, For Official Use Only information, STINFO, or any other information that violates Operations Security.	☐	☐	☐
•	**Notices and Banners**			
14.	Is a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web site? (Ref: DoD Policy, 25 Nov 98, Part I, para 5.5.3, Part II, para 7 and Part V para 4.	☐	☐	☐
15.	Has the appropriate legal authority approved the text of the privacy and security notice for publicly accessible Web sites? Ref: DoD Policy, 25 Nov 98, Part V, para 4.	☐	☐	☐

ITEM (Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)	Y	N	N/A
16. Are flashy graphics or other indicators that create a misconception of danger avoided in association with the privacy and security notice? Ref: DoD Policy, 25 Nov 98, Part II, para 7.	☐	☐	☐
17. Is the required DoD warning notice presented on at the home page of all public sites? The following text **must** be used: *"This Government Computer System is provided as a public service by the (name of the organization). It is intended for use by the public for viewing and retrieving information only. Unauthorized attempts to upload information or change information on this service are strictly prohibited and are punishable under the Computer Fraud and Abuse Act of 1986. Unless otherwise indicated, all information on this system is public information and is available to copy or distribute."*	☐	☐	☐
18. Is the required DoD warning notice presented on at least the home page of all restricted sites? Use the following text as default, if a specific warning notice is not required. *"Official U.S. Government system for authorized use only. Do not discuss, enter, transfer, process, or transmit classified/ sensitive national security information of greater sensitivity than that for which this system is authorized. Use of this system constitutes consent to security testing and monitoring. Unauthorized use could result in criminal prosecution."*	☐	☐	☐
19. Does each page of a Web site restricted from public access clearly state its restriction? The following words should be considered: *"This site is intended for the use of the Defense Distribution Center [or more restrictive audience] only. The content of this site should not be reproduced or redistributed to a wider audience without coordination with the Content Manager and the DDC Command Affairs Office."*	☐	☐	☐
20. If the Web site collects any information on usage or other log files, are visitors notified of what information is collected, why it is collected and how it is used? Ref: DoD Policy, 25 Nov 98, Part II, para 7.	☐	☐	☐
• **Graphics and Link Standards**			
21. Has a reasonable effort been conducted to validate the accuracy of the information and the validity of the links? Ref: DoD Policy, 25 Nov 98, Part II, para 3.8.1. and 3.8.2.	☐	☐	☐
22. Do home pages only point to parent commands or subordinate units, in most cases?	☐	☐	☐
23. Links to non-DoD Web resources should support the organization's mission. Are they periodically reviewed to ensure continued suitability and removed when appropriate? Ref: DoD Policy, 25 Nov 98, Part II, para 8.1.1.	☐	☐	☐
24. Are only text links or hyperlinked text provided to direct visitors to software download sites? (Graphics or logos depicting companies/products shall not appear on publicly accessible Web sites.) Ref: DoD Policy, 25 Nov 98, Part II, para 8.1.4.	☐	☐	☐
25. When external links to non-government Web sites are included, is a disclaimer made as suggested in the reference? (This declaimer may appear on the page or pages listing external links or through an intermediary "exit notice" page generated by the machine.) Ref: DoD Policy, 25 Nov 98, Part II, para 8.1.7., 8.2. The following is a suggested text: *"The appearance of hyperlinks does not constitute endorsement by the Department of Defense of this Web site or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the Department of Defense does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site."*	☐	☐	☐
26. Are links to DoD newspapers and civilian enterprise publications only authorized if advertising is removed? If advertising is included, has the appropriate disclaimer been made? Ref: DoD Policy, 25 Nov 98, Part II, para 8.3.	☐	☐	☐

NO.	ITEM	Y	N	N/A
27.	Are only non-copyrighted material, text, clip art, hypertext links, images and sound or video clips used, provided they directly relate to the mission? Ref: DoD Policy, 25 Nov 98, Part II, para 2.2.	☐	☐	☐
	• Commercial Endorsement	☐	☐	☐
28.	Are product endorsements or preferential treatment of any private organization prohibited from publicly accessible DoD Web sites? Ref: DoD Policy, 25 Nov 98, Part II, para 3.5.6.	☐	☐	☐
29.	Do publicly accessible DoD Web sites not require or encourage users to choose any specific browser? Ref: DoD Policy, 25 Nov 98, Part II, para 8.1.4.	☐	☐	☐
30.	Has the incorporation of non-standard or browser specific features into Web pages been evaluated in light of the potential security risks and interoperability? (Use of these items should be avoided. They could imply an endorsement of the feature and product.) Ref: DoD Policy, 25 Nov 98, Part II, para 11.2.	☐	☐	☐
31.	If "frames" technology is used when connecting to external sites, has legal counsel concerning trademark and copyright issues been performed? Ref: DoD Policy, 25 Nov 98, Part II, para 8.1.5.	☐	☐	☐
32.	Where "frames" technologies are used, do Web site owners ensure that "frames" are not continued when links external to the site are activated?	☐	☐	☐
33.	Is official information about NAF activities incorporated in official DoD Web sites only when no commercial sponsorships or advertisements are included? Ref: DoD Policy, 25 Nov 98, Part II, para 10.1.1.	☐	☐	☐
	• Information Review Policies			
34.	Has the Content Manager (POC for the material) ensured appropriate offices reviewed the material, and identified security and access controls before information is posted on the Internet? Has the release of information by the releasing authority been documented? Ref: DDC Directive 5230.9	☐	☐	☐
35.	Does OMB approve on-line surveys or requests for identical information from ten or more members of the public? (Forms for general solicitations of comments that do not seek responses to standard questions, such as common opinion-based feedback forms and e-mail links, do not require OMB clearance.) Ref: DoD Policy, 25 Nov 98, Part II, para 12.1.	☐	☐	☐
	• Restricted Site Standards (Additional)			
36.	Have access controls as contained in the reference been applied as appropriate for information that must be protected/restricted? Ref: DoD Policy, 25 Nov 98, Part V, para 3. (Users must provide a letter stating the exact restrictions required.)	☐	☐	☐
37.	Does the Content Manager maintain access lists?	☐	☐	☐
38.	Do errors generated by public attempts to access restricted pages redirect the public to the root public page and not include language like "Access Denied" or "Forbidden"? (The redirection should be as transparent as possible to the public.	☐	☐	☐
	• Documentation or Other Standards			
39.	Has the NAF maintained a completed "Internet Release Package" in their official files, to include documentation of the process used to review the information destined for public release?	☐	☐	☐
40.	Do NAF activities follow the specific guidance as specified in the DoD Policy? Ref: DoD Policy, 25 Nov 98, Part II, para 10.1.	☐	☐	☐

DDC World Wide Web Page Request

Name: _____ Date: _____

Telephone Number: _____ Organization/Office: _____

Fax Number: _____ E-mail Address: _____

URL name recommended: _____

CONTENT MANAGER Responsible for keeping Page current:
_____

Access type: _____ PUBLIC _____RESTRICTED

   If RESTRICTED, who is *target audience*: _____

   If PUBLIC, for what purpose_____

Page DESCRIPTION (Please be descriptive. Provide information relating description of *content*, major features or main items of interest on your proposed page. Used additional space to provide examples for clarification):

Key Words (Descriptive terms to aid users in locating resources):

Page Approved / Disapproved

Reviewed by DDC Web Master: _____Yes _____No

Signature: _____

Reviewed by DDC Command Affairs Officer: _____Yes _____No

Signature: _____

Comments, if ***disapproved*** for Internet: